BAROMÈTRE ESET DE LA CYBERSÉCURITÉ

AU CANADA 2018

« Plus de 80 pour cent des Canadiens interrogés croient que les risques d'être victime d'un cybercrime augmentent. »

« Neuf Canadiens sur dix considèrent la cybercriminalité comme un grave défi pour la sécurité du pays, davantage que le terrorisme, la corruption et d'autres activités criminelles. »

ENJOY SAFER TECHNOLOGY™

PRÉFACE

Le Baromètre de la cybersécurité au Canada d'ESET est une enquête d'opinion publique sur la cybersécurité et la cybercriminalité. L'enquête a été menée parce qu'il existe une pénurie de recherches contemporaines quantifiant les attitudes du public à l'égard de la cybercriminalité et son expérience dans ce domaine. Pourtant, l'appui du public aux efforts de cybersécurité, y compris la dissuasion de la cybercriminalité, est essentiel pour préserver les avantages des technologies numériques sur lesquelles nous comptons maintenant.

En tant qu'entreprise de logiciels de sécurité ayant trois décennies d'expérience dans la lutte contre l'abus criminel des systèmes d'information, ESET comprend que les personnes sont l'un des trois facteurs clés impliqués dans la lutte contre la cybercriminalité, les deux autres étant les processus et la technologie. Les gens sont victimes de la cybercriminalité. Les gens élisent les politiciens qui déterminent la politique en matière de cybercriminalité. Les gens paient une grande partie de la facture fiscale pour les efforts d'application de la loi visant à réduire la cybercriminalité. Savoir ce que le public pense de la cybercriminalité et de la cybersécurité est essentiel pour l'élaboration d'une politique efficace en matière de cybercriminalité et indispensable au succès des efforts de la société en matière de cybersécurité. Pour plus d'informations à ce sujet, consultez l'article *Why ask the public about cybercrime and cybersecurity?* (ou *Pourquoi interroger le public sur la cybercriminalité et la cybersécurité*), de Stephen Cobb, chercheur en sécurité d'ESET.

Pour le Baromètre ESET de la cybersécurité 2018, un échantillon de 3 500 personnes a été utilisé (1 000 au Canada et 2 500 aux États-Unis). Le rapport américain paraîtra séparément. Un rapport axé sur les comparaisons entre pays - englobant l'Amérique du Nord et les 28 pays de l'UE - sera également publié. La répétition des enquêtes en 2019 produira des données longitudinales sur les deux continents.

Le baromètre ESET de la cybersécurité s'inspire d'études antérieures menées par l'Union européenne (UE) et publiées sous le titre « Eurobaromètre spécial : Cybersécurité ». L'UE a mené quatre de ces études - la plus récente a été publiée en 2017 - et elles fournissent des recherches longitudinales dans 28 pays sur la base d'un échantillon de 1 000 personnes dans chaque pays. Cette recherche a le potentiel d'aider un large éventail d'acteurs de la cybersécurité, y compris les décideurs, les consommateurs, les entreprises et les agences gouvernementales. Le Baromètre de la cybersécurité d'ESET étend les avantages potentiels de ce type de recherche à l'Amérique du Nord.

MÉTHODOLOGIE

Dans le cadre de cette enquête, 1 000 adultes canadiens ont été sondés en utilisant les standards de méthodologie de l'IVTF (CAWI), avec un échantillonnage aléatoire basé sur l'âge, le sexe et le lieu de résidence. Il a été réalisé pour ESET en septembre 2018 par MNFORCE, en utilisant le panel Research Now SSI.

TABLE DES MATIÈRES

1. SOMMAIRE EXÉCUTIF

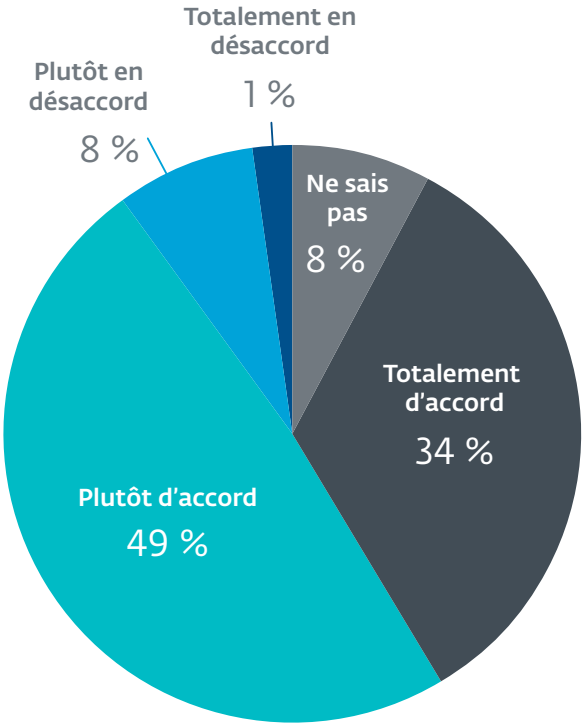
Les résultats du sondage montrent que les Canadiens sont très préoccupés par la cybersécurité; plus de quatre sur dix estiment que le risque de devenir victime d'un cybercrime augmente.

Si le nombre de personnes se déclarant préoccupées par la cybercriminalité est considérablement plus élevé que le nombre de personnes déclarant avoir été victimes de cybercriminalité, ces niveaux de préoccupation devraient néanmoins être pris très au sérieux par les entreprises qui comptent sur la confiance des consommateurs dans Internet.

Les organismes gouvernementaux, tels que les services de détection et de répression, devraient également prendre note de la réduction de la cybercriminalité et affecter leurs ressources à cette fin dans la mesure du possible.

Il est frappant de constater que neuf Canadiens sur dix considèrent maintenant la cybercriminalité comme un grave danger pour la sécurité intérieure du Canada. En outre, il a été constaté que le niveau de préoccupation concernant la cybercriminalité dépassait celui lié au terrorisme, à la corruption et à d'autres activités criminelles graves. Cela donne à penser qu'un réalignement des ressources pourrait s'avérer nécessaire. En effet, moins de la moitié des Canadiens interrogés estiment que les autorités en font assez pour lutter contre la cybercriminalité. Le gouvernement a reçu de meilleures notes pour ses efforts dans la lutte contre le terrorisme et le trafic d'armes.

Le Baromètre de la cybersécurité d'ESET indique clairement que les Canadiens estiment qu'il y a trop de cybercriminalité et pas assez de cybersécurité pour justifier l'adoption complète de la technologie en ligne. Dans la mesure où cette situation entrave les progrès et menace les avantages promis de la transformation numérique, une action concertée des organismes gouvernementaux et des entreprises pour améliorer cette situation semble urgente.



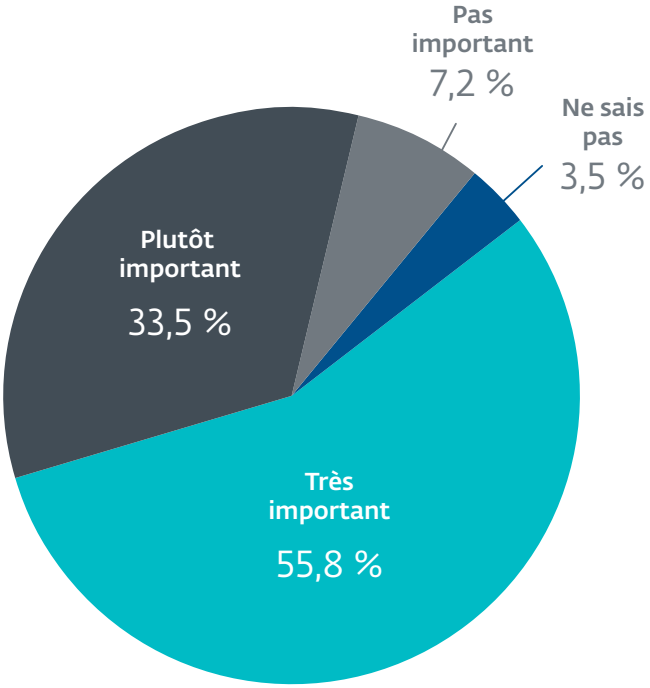
Êtes-vous d'accord avec l'affirmation suivante :
«Je crois que le risque de devenir victime d'un cybercrime augmente»?

2. LA CYBERCRIMINALITÉ, MENACE À LA SÉCURITÉ

Le Baromètre de cybersécurité d'ESET révèle que la plupart des Canadiens considèrent maintenant la cybercriminalité comme un défi important pour la sécurité intérieure du Canada, neuf sur dix disant qu'elle est soit très importante (55,8 %) ou assez importante (33,5 %).

Pour mettre les choses en perspective, les Canadiens considèrent que la cybercriminalité pose davantage un défi à la sécurité intérieure qu'un certain nombre d'autres activités criminelles graves, comme le terrorisme, la traite des personnes ou le blanchiment d'argent.

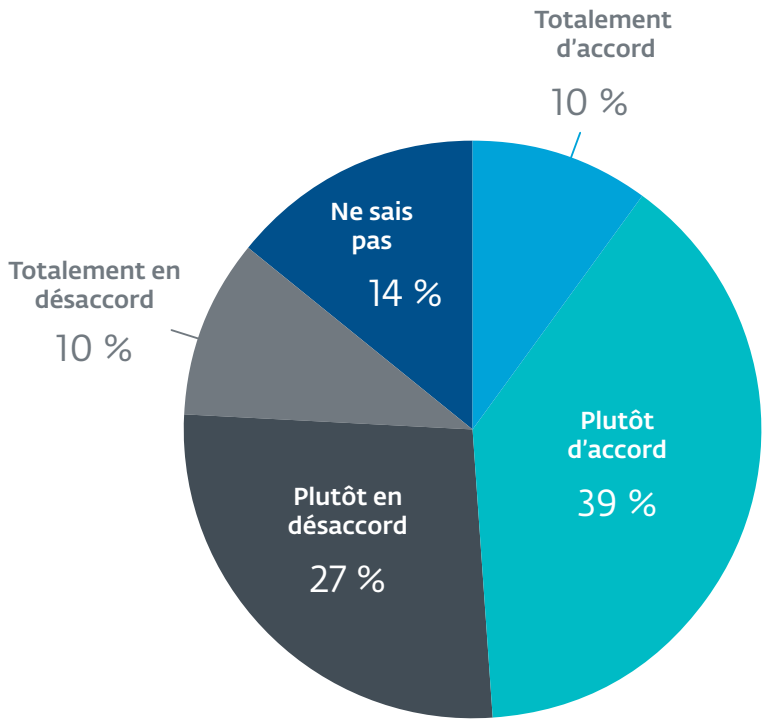
Cette perception de la cybercriminalité semble être largement partagée à travers le Canada, bien que la région de l'Atlantique ait exprimé la plus grande préoccupation (le nombre de répondants de cette région qui ont dit que la cybercriminalité n'était pas très importante était nul).



Quelle est l'importance de la cybercriminalité en tant que défi pour la sécurité intérieure du Canada?

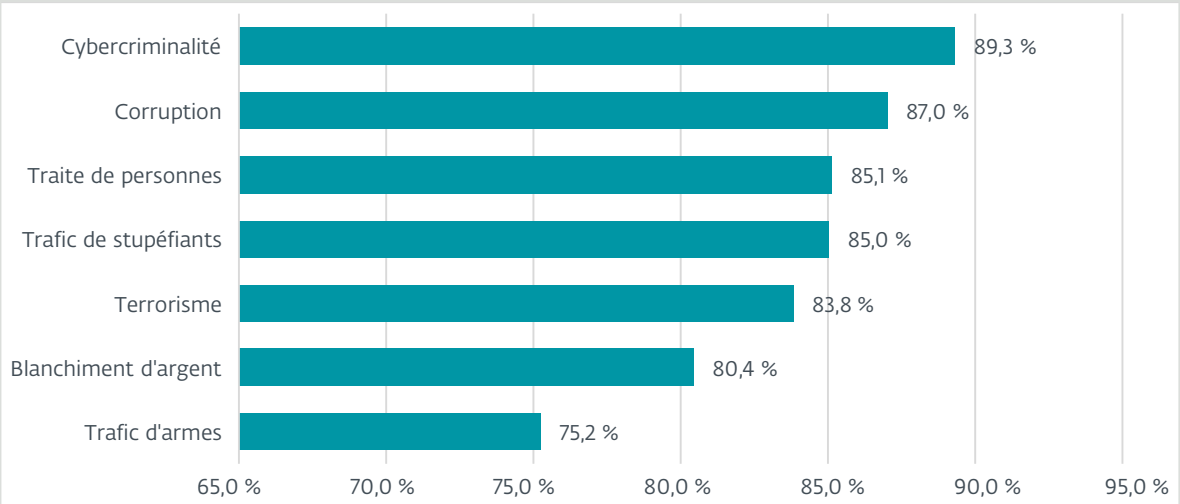
Deux facteurs contribuent à ce niveau élevé de préoccupation à l'égard de la cybercriminalité : les expériences personnelles de la cybercriminalité et les perceptions que les gens ont de la réaction (ou de l'absence de réaction) du gouvernement face à ce problème. Les données de l'enquête portent sur ces deux facteurs.

Un peu moins de la moitié des répondants canadiens pensent que les autorités policières en font assez pour lutter contre la cybercriminalité.



Bien que cela soit décevant - et puisse bien contribuer aux niveaux élevés de préoccupation à l'égard de la cybercriminalité - c'est néanmoins mieux que la perception au sud de la frontière.

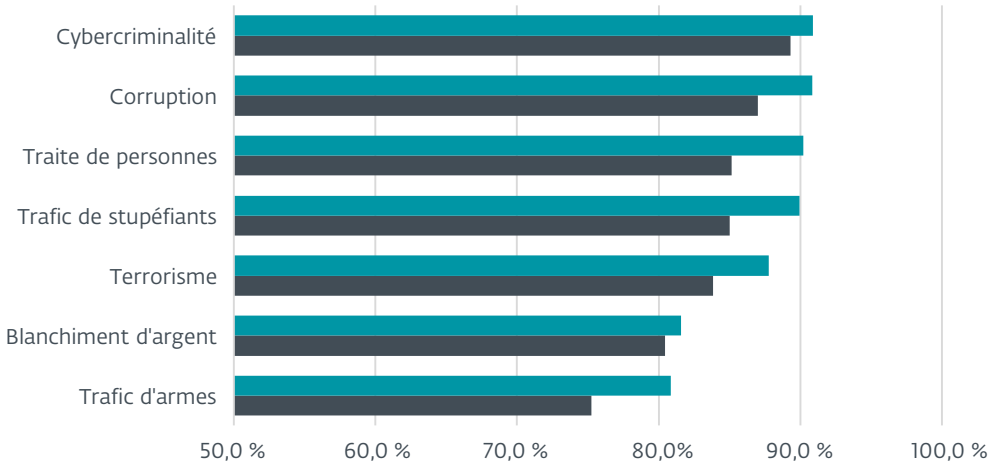
Seuls 44 % des répondants américains interrogés étaient d'accord pour dire que les autorités de leur pays en faisaient assez pour lutter contre la cybercriminalité.



Importance de l'activité criminelle en tant que défi à la sécurité intérieure du Canada
(pourcentage de répondants ayant sélectionné « Assez important » ou « Très important »)

La plupart des professionnels de la cybersécurité s'accordent à dire que la lutte contre la criminalité dans le cyberespace est très différente de la lutte contre la criminalité dans l'espace physique, et beaucoup plus difficile. Pour que la police et les autres autorités chargées de l'application de la loi gagnent du terrain contre les criminels dans le cyberespace, il faut investir sérieusement dans les compétences et les ressources, tout en indiquant clairement que la lutte contre la cybercriminalité est une priorité.

Selon le sondage, les Canadiens ont tendance à penser que le gouvernement fait un meilleur travail contre le terrorisme et le trafic d'armes que contre la cybercriminalité ou la corruption. Cela peut se refléter dans la façon dont les Canadiens ont répondu lorsqu'on leur a demandé d'évaluer l'importance de sept types d'activités criminelles en tant que défis à la sécurité intérieure.

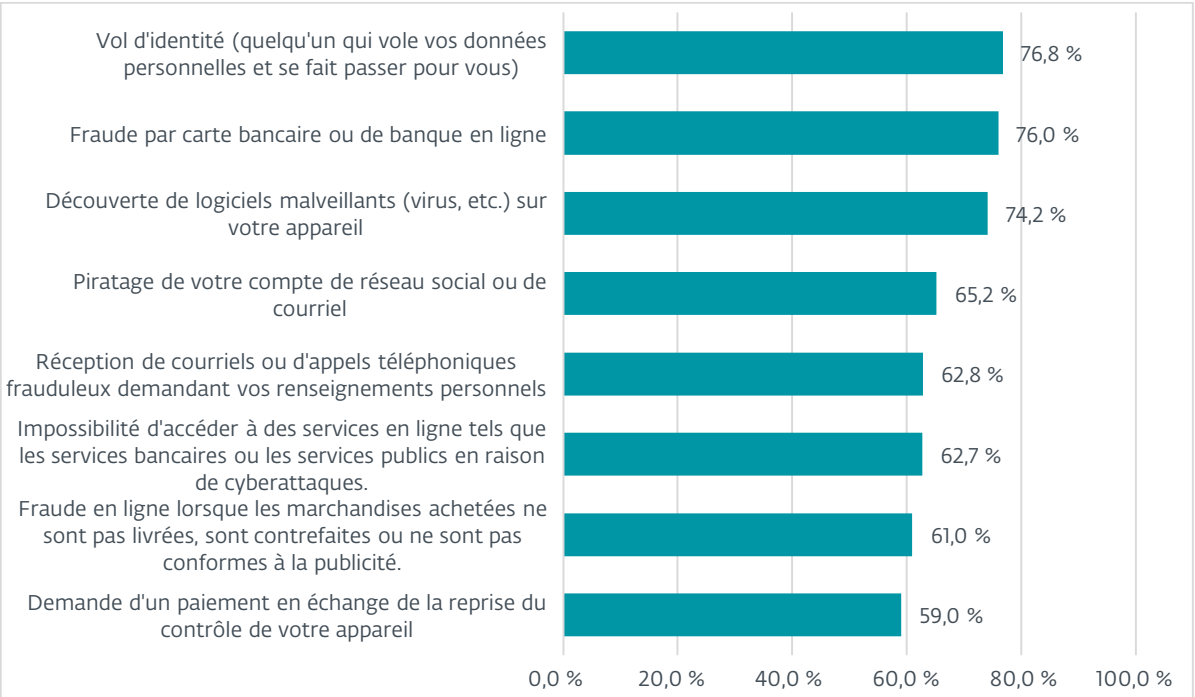


Importance de diverses activités criminelles en tant que défis à la sécurité intérieure de votre pays (pourcentage de répondants qui ayant choisi « Assez important » ou « Très important »)

Les Canadiens ne sont pas les seuls à placer la cybercriminalité en tête de liste. Aux États-Unis, les personnes interrogées considèrent également la cybercriminalité comme le défi le plus important, mais à un degré encore plus élevé. Toutefois, bien que les Canadiens soient moins préoccupés par toutes ces activités criminelles que leurs voisins du Sud, il est intéressant de constater que l'écart entre les préoccupations des Canadiens et celles de leurs voisins du Sud à l'égard de la cybercriminalité est relativement faible.

3. PRÉOCCUPATIONS EN MATIÈRE DE CYBERSÉCURITÉ

Le Baromètre de la cybersécurité d'ESET a demandé aux Canadiens dans quelle mesure ils étaient préoccupés par les diverses formes d'activités cybercriminelles comme le piratage de leur compte de courriel ou de réseau social, la découverte de logiciels malveillants sur leur ordinateur ou le fait qu'on leur demande un paiement en échange du contrôle de leur appareil (rançongiciel).



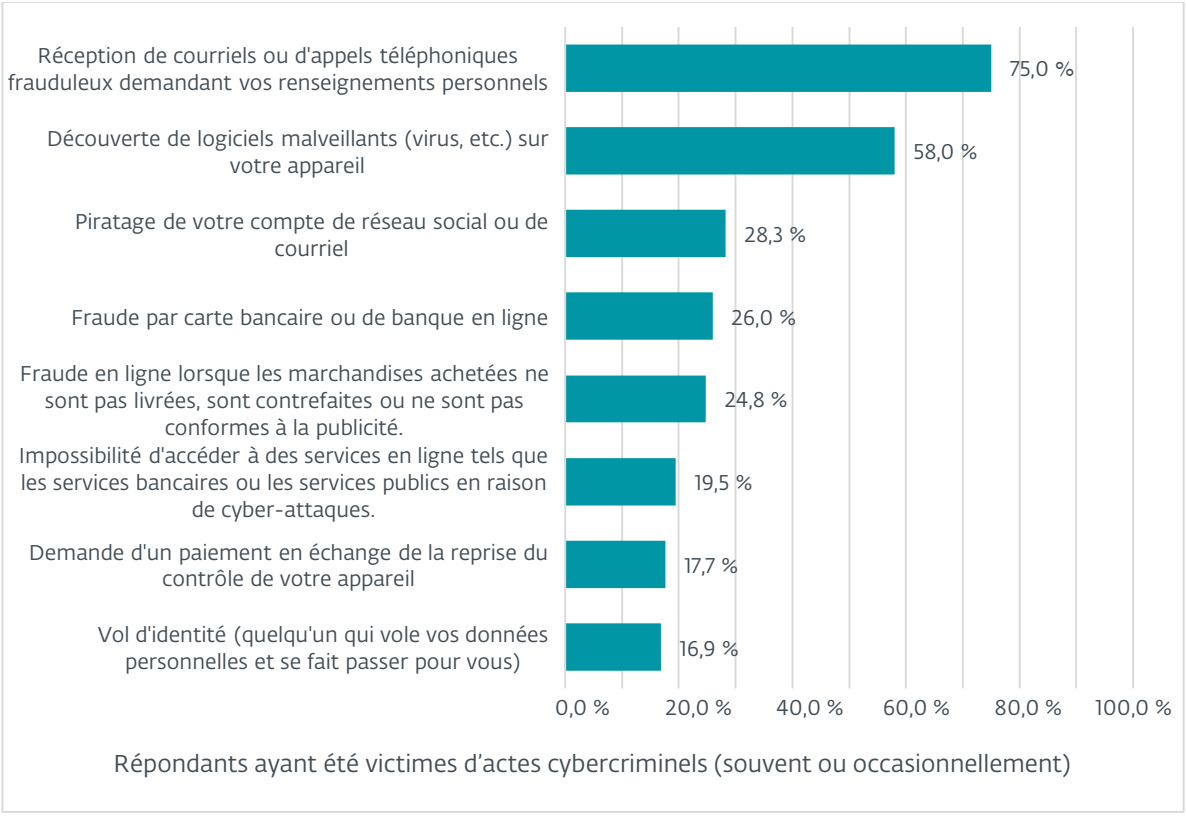
Pourcentage de personnes interrogées affirmant être préoccupées par les activités cybercriminelles (ayant répondu « Très préoccupé » ou « Assez préoccupé »)

Les deux graphiques suivants explorent ces données, qui indiquent que la plus grande préoccupation est le vol d'identité, défini dans l'enquête comme « quelqu'un qui vole vos données personnelles et se fait passer pour vous ». Vient ensuite la crainte d'être victime d'une fraude par carte bancaire ou par les services bancaires en ligne. L'infection par des logiciels malveillants vient compléter les trois principales préoccupations.

Dans l'ensemble, ces réponses aux questions portant sur des préoccupations précises en matière de cybersécurité peuvent aider à expliquer pourquoi les Canadiens pensent que la cybercriminalité est un si gros problème : les huit questions concernent plus de 60 % des répondants, à l'exception du fait qu'on leur demande un paiement en échange du contrôle de leur appareil, qui a obtenu 59 %.

(Notez que demander un paiement « en échange de la reprise du contrôle de votre appareil » représente une façon de décrire un rançongiciel, mais la question de l'enquête a été développée - et suivie dans l'UE - avant que le terme rançongiciel (ou logiciel rançon) ne soit largement utilisé. Il est possible que plus de gens auraient exprimé leur inquiétude si ce terme avait été utilisé.)

Les niveaux d'inquiétude à l'égard de la possibilité d'être victime d'un acte criminel ne reflètent peut-être pas directement l'ampleur de la criminalité, de sorte que l'enquête pose aussi directement la question : « Combien de fois avez-vous vécu ou avez-vous été victime des situations suivantes? » L'enquête suit les mêmes catégories que dans les questions sur les niveaux de préoccupation. Les résultats montrent qu'au Canada, plus de la moitié des répondants ont été victimes d'actes criminels entrant dans les deux catégories suivantes : les demandes frauduleuses de renseignements personnels et les logiciels malveillants.



Répondants ayant été victimes d'actes cybercriminels (souvent ou occasionnellement)

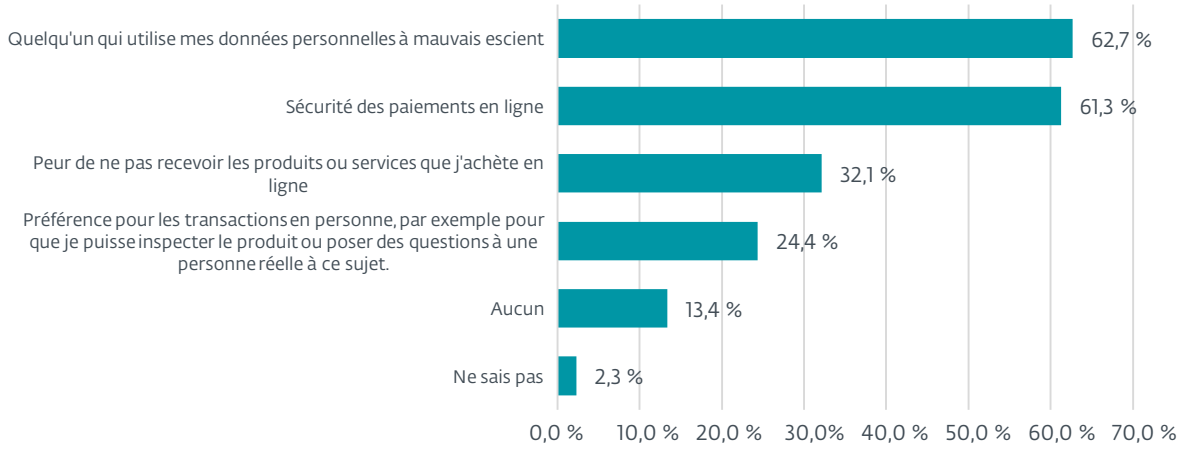
Du point de vue de la criminologie, il est intéressant de noter que le vol d'identité était l'élément le moins connu mais le plus redouté parmi ceux qui ont été présentés. Cependant, de telles relations inverses ne sont pas sans précédent dans la recherche sur la criminalité. La crainte de crimes spécifiques peut être amplifiée par une couverture médiatique importante et une défense bien intentionnée des victimes. Cela peut avoir des effets positifs, comme attirer des ressources pour s'attaquer au problème et encourager les victimes potentielles à adopter des comportements qui réduisent la criminalité.

Bien sûr, certains crimes sont plus dramatiques que d'autres en termes d'impact sur la vie des gens. Par exemple, des preuves anecdotiques suggèrent que le vol d'identité peut être très troublant pour les gens, causant un impact psychologique plus important que certaines autres formes de criminalité numérique.

Interrogés au sujet de diverses préoccupations en matière de cybersécurité liées aux services bancaires et aux achats en ligne, plus de trois Canadiens sur cinq ont indiqué qu'ils s'inquiétaient de l'utilisation abusive des données personnelles fournies dans les transactions en ligne.

Bien que le Canada ait travaillé d'arrache-pied pour devenir un chef de file en matière de protection de la vie privée numérique, ces résultats donnent à penser que les entreprises avec lesquelles les Canadiens font affaire en ligne pourraient mieux rassurer les clients en ligne du Canada au sujet de la protection des renseignements personnels qu'elles offrent. On pourrait également soutenir qu'une diminution des manchettes sur les atteintes à la protection des données contribuerait à améliorer la confiance.

Trois Canadiens sur cinq se sont également dits préoccupés par la sécurité des paiements en ligne. Encore une fois, cela pourrait être interprété comme un appel aux commerçants en ligne pour qu'ils améliorent leur position de sécurité et démontrent qu'ils prennent au sérieux la sécurité des transactions en ligne.



Quelles sont vos préoccupations, le cas échéant, au sujet de l'utilisation d'Internet pour des gestes comme les services bancaires en ligne ou l'achat d'articles en ligne?

Soulignons que les préoccupations au sujet de l'utilisation abusive des données personnelles dans les transactions en ligne étaient beaucoup plus faibles au Québec (57 %) que dans le reste du Canada. En Amérique du Nord en général, on se préoccupe moins de la non-livraison des biens et services achetés en ligne que de la sécurité des paiements en ligne, mais les Canadiens sont plus préoccupés par la non-livraison des achats en ligne que leurs homologues américains (32 % versus 24 %).

Dans les provinces maritimes, la préférence pour l'exécution des transactions en personne en réponse aux préoccupations liées à la sécurité en ligne était beaucoup plus élevée (36 %) que dans le reste du Canada. Malgré cette préférence, les Maritimes ont signalé un niveau moyen d'activité en ligne dans la catégorie « achat de biens et services », comme le montre ce tableau.

Quelles activités parmi les suivantes faites-vous en ligne?	RÉGION				
	Ontario	Maritimes	Ouest	Québec	Canada
Banque en ligne	89,0 %	87,5 %	84,3 %	85,2 %	86,6 %
Achat de biens ou de services (vacances, livres, musique, etc.)	79,5 %	75,0 %	74,3 %	70,0 %	75,4 %
Vente de biens ou de services	33,2 %	40,3 %	31,3 %	32,1 %	32,9 %
Utilisation des réseaux sociaux en ligne	79,5 %	87,5 %	72,0 %	74,7 %	76,7 %
Envoi ou réception de courriels	90,8 %	93,1 %	93,0 %	89,9 %	91,4 %
Lire les nouvelles	78,8 %	80,6 %	80,3 %	72,6 %	77,9 %
Jouer à des jeux	54,0 %	63,9 %	52,3 %	52,3 %	53,8 %
Regarder la télé	48,3 %	50,0 %	44,3 %	48,5 %	47,3 %
Autre	2,0 %	1,4 %	2,7 %	2,5 %	2,3 %
Ne sais pas	0,5 %	0,0 %	0,3 %	0,4 %	0,4 %

Les préoccupations liées à l'utilisation d'Internet ont également été évaluées au moyen d'une question du sondage qui demandait aux répondants s'ils étaient d'accord ou en désaccord avec cet énoncé : « Je suis préoccupé par le fait que mes informations personnelles en ligne ne sont pas sécurisées par les sites Web. » Malheureusement, un Canadien sur quatre qui a répondu au sondage a dit qu'il était tout à fait d'accord. Presque la moitié d'entre eux étaient d'accord. Compte tenu de la mesure dans laquelle les entreprises et les organismes gouvernementaux en sont venus à utiliser Internet comme outil de communication et d'interaction avec le public, ces chiffres devraient être inquiétants.

Le sondage questionnait également les gens sur leur opinion par rapport à cet énoncé : « Je suis préoccupé par le fait que mes informations personnelles en ligne ne sont pas sécurisées par les autorités publiques ». Les deux tiers des répondants canadiens, ce qui est décevant, étaient généralement d'accord (45 %) ou tout à fait d'accord (22 %). Dans l'ensemble, la préoccupation était la plus faible au Québec (64 %) et la plus élevée dans la région des Maritimes (72 %).

Lorsqu'il s'agit d'améliorer la cybersécurité et de faire face aux risques de cybercriminalité, il est utile de connaître le degré de confiance que les gens ont dans leur capacité à comprendre le problème. Le Baromètre de cybersécurité d'ESET a révélé que les deux tiers des Nord-Américains interrogés se considéraient bien informés sur les risques de la cybercriminalité (soit « Assez bien informés » ou « Très bien informés »). Toutefois, la confiance était plus élevée aux États-Unis (70 %) qu'au Canada (62 %).

En comparaison, lorsque cette même question a été posée aux résidents des 28 pays de l'UE en 2017, le pourcentage total de personnes se considérant bien informées n'était que de 46 % pour l'ensemble de la région. Des variations considérables ont notamment été observées entre les pays (allant de 27 % en Bulgarie à 76 % au Danemark). Comme le montre le tableau suivant, il y a eu des variations régionales considérables au Canada. Les régions des Maritimes et de l'Ouest se considéraient moins bien informées, tandis que les gens de l'Ontario semblaient plus confiants.

Dans quelle mesure vous considérez-vous informé sur les risques de la cybercriminalité?		RÉGION				
		Ontario	Maritimes	Ouest	Québec	Canada
	Très bien informé	13,0 %	12,5 %	5,7 %	13,1 %	10,8 %
	Assez bien informé	51,4 %	44,4 %	54,7 %	47,7 %	51,0 %
	Pas très bien informé	29,7 %	37,5 %	31,7 %	33,3 %	31,7 %
	Pas du tout informé	3,8 %	2,8 %	5,0 %	3,0 %	3,9 %
	Ne sais pas	2,0 %	2,8 %	3,0 %	3,0 %	2,6 %

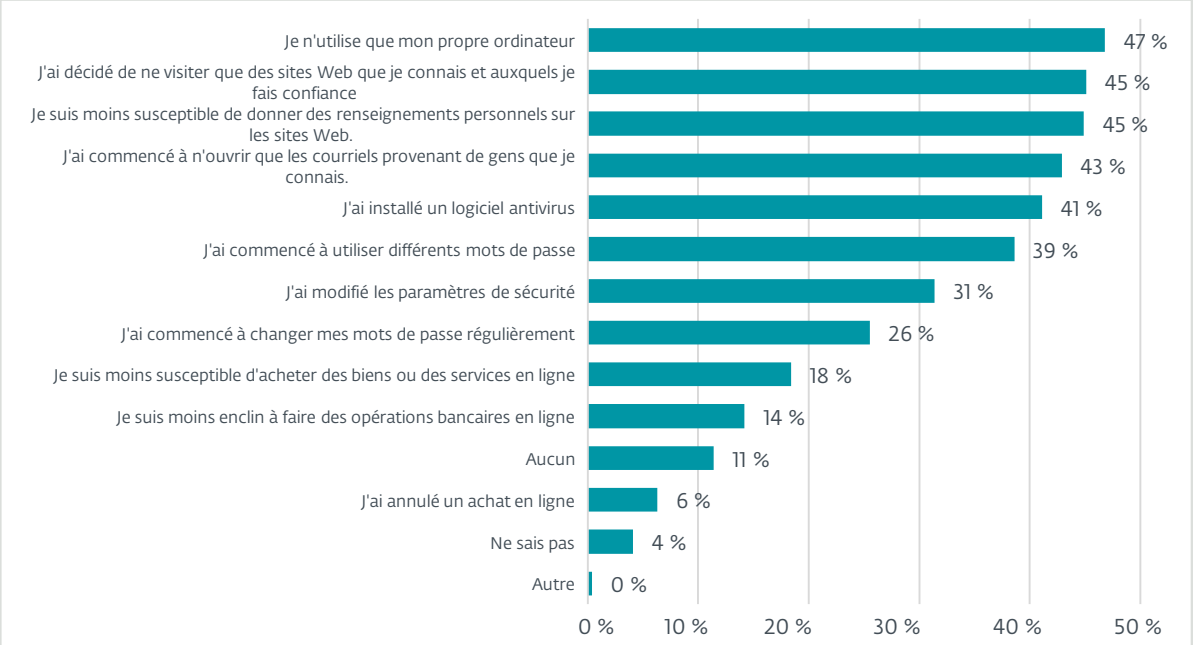
Être bien informé sur la cybercriminalité est une chose; croire que l'on peut se protéger contre la cybercriminalité en est une autre. Le sondage a révélé que les deux tiers des Canadiens semblent confiants à cet égard, d'accord avec l'affirmation suivante : « Je suis capable de me protéger suffisamment contre la cybercriminalité, par exemple en utilisant un logiciel antivirus. » Inversement, l'autre tiers peut représenter un potentiel de croissance du marché pour les fournisseurs de sécurité.

Je suis capable de me protéger adéquatement contre la cybercriminalité, par exemple en utilisant un logiciel antivirus.	RÉGION				
	Ontario	Maritimes	Ouest	Québec	Canada
Totalement d'accord	16,6 %	15,3 %	14,3 %	17,3 %	16,0 %
Plutôt d'accord	52,4 %	41,7 %	50,7 %	47,7 %	50,0 %
Plutôt en désaccord	18,4 %	25,0 %	17,7 %	19,4 %	18,9 %
Totalement en désaccord	4,6 %	2,8 %	2,7 %	3,4 %	3,6 %
Ne sais pas	7,9 %	15,3 %	14,7 %	12,2 %	11,5 %

4. RIPOSTE EN MATIÈRE DE CYBERSÉCURITÉ

Au cours des trois dernières années, les Canadiens ont pris diverses mesures pour des raisons de sécurité et de protection des renseignements personnels lorsqu'ils utilisent Internet, qu'il s'agisse de n'utiliser que leur propre ordinateur ou de changer leur mot de passe. Plus d'un tiers des personnes interrogées ont ajusté leurs paramètres de sécurité et installé un logiciel antivirus.

Les entreprises qui comptent beaucoup sur les transactions par Internet devraient noter le pourcentage de personnes qui ont déclaré qu'elles sont moins susceptibles de magasiner ou de faire des opérations bancaires en ligne pour des raisons de sécurité et de confidentialité (18 % et 14 %, respectivement). Bien que les pourcentages ne soient pas élevés, ils représentent certainement des occasions perdues pour les détaillants et les entreprises financières. Les spécialistes du marketing devraient également noter que près de la moitié des Canadiens ont choisi de donner moins de renseignements personnels sur les sites Web.



Mesures prises au cours des trois dernières années en raison de problèmes de sécurité et de protection de la vie privée lors de l'utilisation d'Internet

Afin d'évaluer les priorités des gens en matière de sécurité, on a posé la question aux répondants du Baromètre de la cybersécurité d'ESET : « Avez-vous changé votre mot de passe pour accéder à votre (vos) compte(s) pour l'un des services en ligne suivants au cours des 12 derniers mois? » Sept catégories de comptes ont été présentées et, de toute évidence, les comptes de courriel représentaient la principale préoccupation, en supposant qu'un changement de mot de passe reflète un problème de sécurité ou une priorité accrue. ne. Encore une fois, cela pourrait être interprété comme un appel aux commerçants en ligne pour qu'ils améliorent leur position de sécurité et démontrent qu'ils prennent au sérieux la sécurité des transactions en ligne.

Avez-vous changé votre mot de passe pour accéder à votre (vos) compte(s) pour l'un des services en ligne suivants au cours des 12 derniers mois?	Ontario	Maritimes	Ouest	Québec	Canada
Courriel	61,6 %	73,6 %	55,3 %	55,3 %	59,1 %
Réseaux sociaux en ligne	44,0 %	52,8 %	35,0 %	45,1 %	42,2 %
Sites d'achat en ligne	37,1 %	38,9 %	32,0 %	29,5 %	33,9 %
Banque en ligne	54,0 %	59,7 %	50,7 %	46,8 %	51,7 %
Jeux en ligne	14,8 %	18,1 %	12,0 %	13,9 %	14,0 %
Sites Web des services publics	18,2 %	19,4 %	14,7 %	16,0 %	16,7 %
Autre	2,3 %	1,4 %	3,0 %	3,0 %	2,6 %
Aucun	17,1 %	5,6 %	20,3 %	20,7 %	18,1 %

5. DISCUSSION

La cybersécurité consiste à protéger les technologies numériques - dont nous dépendons aujourd'hui si fortement - contre les criminels qui cherchent à abuser de ces technologies à leurs propres fins. Le soutien du public aux efforts visant à réduire la cybercriminalité est essentiel aux efforts de la société pour préserver les avantages des technologies numériques. C'est pourquoi il est si important de savoir ce que le public pense de la cybercriminalité et de la cybersécurité, ce que l'UE a reconnu en créant le Baromètre européen de la cybersécurité.

Les données récoltées dans le cadre de ce projet ont non seulement aidé à éclairer les décisions politiques dans les pays de l'UE, mais elles ont également apporté une contribution précieuse aux projets de commercialisation. Des chercheurs universitaires ont utilisé les données pour analyser la relation entre l'expérience de la cybercriminalité et l'adoption des technologies en ligne.

Ni le gouvernement canadien ni le gouvernement américain ne semblent avoir ressenti le besoin d'entreprendre des enquêtes similaires auprès de leurs citoyens, se contentant apparemment de laisser les entreprises être la source par défaut de données sur le problème de la cybercriminalité. Cette approche pose plusieurs problèmes. Les résultats de toute enquête sur la cybersécurité menée par une entreprise qui vend des produits et services liés à la sécurité peuvent être accusés de partialité, en particulier si les implications de ces résultats entrent en conflit avec les objectifs des politiciens et des responsables politiques auxquels ils sont présentés.

La même faiblesse peut également toucher le secteur privé. Tout PDG qui ne veut pas croire que le public perçoit la cybercriminalité comme une menace sérieuse peut écarter la recherche commanditée par l'entreprise. L'une des raisons de vouloir ignorer les preuves croissantes d'une crise imminente de cybercriminalité pourrait être la résistance à l'augmentation du coût d'un produit matériel ou logiciel afin de le rendre plus sûr. L'abondance de produits insuffisamment sécurisés ne fait qu'accroître l'incidence de la cybercriminalité.

La principale raison pour laquelle le Baromètre de la cybersécurité d'ESET a été soumis aux mêmes questions que la recherche de l'UE était de réfuter les accusations de partialité. L'enquête a été menée par une firme d'arpentage réputée selon une méthodologie reconnue. Les résultats sont solides et devraient être utilisés par les décideurs qui travaillent sur le problème de la cybercriminalité sans crainte d'être remis en question.

En conclusion, ces résultats suggèrent fortement que, à moins que la cybersécurité et la dissuasion de la cybercriminalité ne soient considérées comme des priorités par les organismes gouvernementaux et les entreprises, le taux d'abus des systèmes et des données continuera d'augmenter, ce qui minera davantage la confiance du public dans la technologie. Cette confiance est vitale pour le bien-être économique du Canada, aujourd'hui et à l'avenir.

Auteur : Stephen Cobb, CISSP